Internet of Things and Cloud Computing
2024, Vol. 12, No. 1, pp. 10-16
https://doi.org/10.11648/j.iotcc.20241201.12

Review Article

The Current Status and Challenges of Cybersecurity Risks

Xudong Sun*

Marketing Center, QI-ANXIN Technology Group Inc, QAX Security Center, Beijing, China

Abstract

Research Context and Aims: The swift expansion of internet technologies has rendered the digital network essential to contemporary life, highlighting the significance of cybersecurity. Network data not only encompasses personal information management and communication but also pertains to the protection of confidential corporate, governmental, and vital national infrastructures. Consequently, cybersecurity has become a critical issue in current society. Frequent occurrences like privacy violations, data thefts, and national security threats underline the critical need for enhanced network defenses and protective measures. *Research Approach*: This study examines the state of cybersecurity by assessing pertinent studies across public databases such as PubMed, CNKI, and CrossRef. It compiles and evaluates significant cybersecurity events including data breaches, malware attacks, and phishing, outlining key security challenges faced by networks. The paper also evaluates the current cybersecurity technologies and methods, pinpointing their effectiveness and limitations in addressing network threats. *Research Findings*: The findings reveal that cyber attackers have refined their methods, employing sophisticated, covert techniques for prolonged periods, which often outpace current defenses. In cases of data breaches, perpetrators frequently utilize precise social engineering or deploy advanced persistent threats (APTs). Additionally, the proliferation of IoT technology has not only obscured the boundaries of cybersecurity but also broadened potential attack vectors. Despite the implementation of security measures like encryption and multi-factor authentication, these can be compromised by managerial or operational oversights. *Research Conclusions*: With the cybersecurity landscape becoming increasingly challenging, future defenses will likely prioritize the adoption of integrated, proactive strategies. It is crucial to foster the development of smart security solutions, such as leveraging artificial intelligence to detect and respond to anomalies. Furthermore, boosting security awareness among users and ensuring standardized practices are imperative. Ultimately, formulating future cybersecurity policies will require a holistic approach, integrating technological, managerial, legal, and educational initiatives to forge a robust network defense architecture.

Keywords

Encryption, Firewall, Vulnerability, Malware, Authentication, Intrusion Detection, Security Awareness Training, Cybersecurity

1. Introduction

In today's digital landscape, cybersecurity plays a pivotal role in safeguarding information and systems against digital threats [1]. As network technologies rapidly evolve, cyberattacks become more frequent and sophisticated [2]. Addressing cybersecurity challenges demands a multifaceted approach, encompassing comprehensive strategies for effective risk mitigation. Establishing robust institutional and policy frameworks is crucial to ensure legal and orderly conduct in

*Corresponding author: vvip161@163.com (Xudong Sun)

Received: 28 May 2024; **Accepted:** 18 June 2024; **Published:** 4 July 2024

Copyright: © The Author(s), 2024. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

cyberspace [3]. This entails reinforcing legislation, overseeing network management practices, and upholding cybersecurity rule of law. Heightened individual, organizational, and national awareness and engagement are imperative for effective cybersecurity [4]. Individuals should enhance their cybersecurity awareness, adhere to standards and guidelines, and actively safeguard personal information [5]. Similarly, businesses and organizations should strengthen internal security measures, establish robust governance systems, and ensure data and network integrity [6-8]. Nationally, there is a need to bolster cybersecurity strategies, allocate resources for research and talent development, and build resilient cybersecurity ecosystems. With the ongoing evolution of technologies like cloud computing and artificial intelligence, cybersecurity faces continual challenges, underscoring the necessity for ongoing innovation and development. Collaboration among individuals, organizations, and nations is essential to confront cybersecurity threats and ensure cyberspace's security and stability [9-12].

2. Research Methodology

In this study, this adopt a comprehensive approach to assess the state of cybersecurity. By analyzing relevant literature from public databases like PubMed, CNKI, and CrossRef, this study delve into the latest developments and trends in cybersecurity. This study compile and scrutinize significant cybersecurity incidents, ranging from data breaches to malware attacks and phishing attempts, to provide a detailed overview of the key security challenges encountered by networks. Furthermore, this study meticulously evaluate the efficacy and constraints of existing cybersecurity technologies and methodologies, aiming to identify their strengths and weaknesses in mitigating network threats. Through this multifaceted analysis, this study aim to offer valuable insights into the current landscape of cybersecurity and inform future strategies for enhancing network security.

3. Results

3.1. Network Security Threats and Targets

In today's digital landscape, network security risks are evolving and diversifying. Here are some prevalent types of network security threats:

Malware: Malicious software, including viruses, worms, and trojans, can infiltrate systems through various means such as infected files or social engineering. These programs are capable of damaging systems, stealing data, or hijacking computer resources, posing significant risks to individuals, businesses, and organizations.

Phishing: Phishing is a common form of social engineering attack where attackers deceive users into providing sensitive information by impersonating legitimate entities. These attacks often occur through email or social media, leading to information leakage and financial losses for victims.

Distributed Denial of Service (DDoS) Attacks: DDoS attacks overwhelm target servers or network devices with a massive volume of fake requests, rendering them inaccessible to legitimate users. Attackers utilize large botnets or other methods to flood servers, causing disruptions to services.

Advanced Persistent Threats (APT): APTs are sophisticated and persistent network attacks orchestrated by organized hacker groups. These attacks, often initiated by state-level organizations, aim to steal critical data or disrupt infrastructure. APTs employ multi-stage attack methods, including vulnerabilities exploitation and social engineering, posing serious threats to network security.

3.2. Network Security Attacks Target Various Entities, Including Individual Users, Businesses, and Governments

Here are the primary network security threats faced by these different targets:

Individual Users: Individual users are targeted for their personal privacy and financial information. Attackers use methods such as phishing emails and malware to steal sensitive data, resulting in financial and reputational losses.

Businesses and Organizations: Businesses and organizations face complex threats to their data, intellectual property, and operations. Attackers may seek to gain access to trade secrets or disrupt business operations, leading to financial losses and reputational damage.

Government and Public Facilities: Governments and public facilities are targeted for sensitive information and infrastructure disruption. Attackers use advanced methods to breach government systems, posing significant security risks and societal impacts.

The diversification of network security threats and targets poses challenges to individuals, businesses, and nations. Addressing these challenges requires collaborative efforts to strengthen security awareness, enhance technical defenses, and establish robust legal frameworks for network security and societal stability.

4. Discussion

4.1. Security Protection Technology Advancements

In the dynamic realm of cybersecurity, the evolution of security protection technologies is vital for safeguarding digital assets and countering cyber threats [13-15]. Here's a closer look at some key innovations in this domain:

Firewalls and Intrusion Detection Systems (IDS): Foundational to network security, firewalls act as gatekeepers between trusted internal networks and external ones, managing

incoming and outgoing traffic based on predefined security protocols [16]. Meanwhile, IDS monitors network or system activities for signs of malicious behavior or policy violations, promptly alerting administrators to potential breaches [17]. Despite being traditional, these tools remain indispensable in thwarting unauthorized access and identifying suspicious activities within networks [18].

Encryption Technology: Encryption plays a pivotal role in protecting data during transmission and storage [19]. By converting information into ciphertext that's only decipherable with the corresponding decryption key, encryption ensures that sensitive data remains shielded from unauthorized access or interception [20]. With the prevalence of cloud computing and remote work, encryption has become increasingly essential in safeguarding confidential information across diverse communication channels and storage platforms.

Multi-Factor Authentication (MFA): MFA enhances authentication security by requiring users to provide multiple forms of verification before gaining access to a system or application [21]. This could involve something they know (like a password), something they possess (such as a smartphone or hardware token), or something they are (like biometric data). By layering authentication, MFA significantly reduces the risk of identity theft and unauthorized access, bolstering overall security measures [22].

Artificial Intelligence and Machine Learning: AI and ML have emerged as potent allies in the battle against cyber threats [23]. These technologies enable automated analysis of vast datasets to detect patterns, anomalies, and potential security breaches in real-time. AI-driven security solutions can identify and respond to cyber threats more efficiently than conventional methods, empowering organizations to proactively mitigate risks and fortify their defense mechanisms [24]. Furthermore, AI and ML algorithms can adapt and evolve in response to evolving threat landscapes, making them invaluable assets in the ongoing fight against cyber adversaries [25]. As organizations navigate the intricate and ever-changing cybersecurity terrain, adopting these advanced security protection technologies is paramount to erecting resilient defense mechanisms and shielding digital assets from sophisticated threats. However, it's imperative to acknowledge that cybersecurity isn't a one-size-fits-all solution [26]. A holistic approach that melds technology, processes, and human expertise is essential to effectively mitigating risks and ensuring the durability of digital infrastructure amidst evolving cyber threats.

4.2. Challenges in Cybersecurity

4.2.1. Information Challenges

Despite the implementation of various security measures, cybersecurity encounters numerous challenges [27]. The rapid pace of technological advancements introduces new and evolving threats to digital security. From the proliferation of Internet of Things (IoT) devices to the adoption of cloud computing and the misuse of artificial intelligence (AI) by malicious actors, the landscape of cyber threats continues to evolve [28]. These emerging threats exploit vulnerabilities in digital infrastructure, posing significant risks to individuals, businesses, and governments worldwide [29]. Addressing these challenges requires proactive measures, including enhanced security protocols, user education initiatives, and regulatory reforms to adapt to the evolving cyber threat landscape.

4.2.2. The Internet of Things (IoT)

The widespread deployment of unprotected IoT devices has opened new avenues for cyberattacks [30]. As IoT devices become increasingly integrated into daily life, including smart homes and industrial systems, the associated security risks are escalating. Hackers exploit vulnerabilities in IoT devices to gain unauthorized access, manipulate data, or launch attacks on interconnected systems [31].

4.2.3. Cloud Computing

While cloud computing offers scalability and cost-effectiveness, it also introduces new security risks [32]. Centralizing data in the cloud raises concerns about data breaches, unauthorized access, and loss of control over sensitive information [33]. Organizations relying on cloud services must address issues related to data privacy, regulatory compliance, and the security of cloud infrastructure [34].

4.2.4. Misuse of Artificial Intelligence

While AI holds promise for enhancing cybersecurity defenses, it also presents challenges when used by malicious actors [35]. Cybercriminals are leveraging AI-driven tools to orchestrate sophisticated attacks, including targeted phishing emails and evasive maneuvers to avoid detection [36]. These AI-powered threats pose significant challenges to traditional cybersecurity measures.

4.2.5. Human Factors

Lack of User Security Awareness. Many users lack basic cybersecurity knowledge, making them vulnerable to cyberattacks [37]. From falling victim to phishing scams to using weak passwords, uninformed users inadvertently compromise the security of their personal devices and sensitive data. Educating users about cybersecurity best practices is essential for cultivating a security-conscious culture and reducing susceptibility to cyber threats.

4.2.6. Internal Threats

Insider threats, whether due to negligence or malicious intent, pose a substantial risk to organizational security. Employees with access to sensitive data may inadvertently expose information through careless actions or intentionally

sabotage systems for personal gain or revenge [38]. Implementing robust access controls, monitoring employee activities, and conducting regular security audits are essential for detecting and mitigating internal threats effectively.

4.2.7. Legal and Regulatory Challenges

Cybersecurity laws and regulations often lag behind technological advancements, creating regulatory gaps and enforcement challenges [39]. Regulatory bodies struggle to keep pace with emerging cyber threats and address cybersecurity issues in a timely manner. Additionally, the transnational nature of cybercrime complicates efforts to track perpetrators and enforce laws across borders [40]. Effective international cooperation mechanisms are necessary to facilitate information sharing, coordinate law enforcement efforts, and prosecute cybercriminals operating globally [41]. Addressing the multifaceted challenges in cybersecurity requires a holistic approach involving technological innovation, user education, organizational policies, and regulatory reforms. By recognizing and actively addressing these challenges, stakeholders can bolster cybersecurity resilience and mitigate evolving threats in today's interconnected digital landscape.

4.3. The Future Trends of Network Security Risk Control

Future trends in network security risk control are shaping the trajectory of development in information technology [42]. In today's digital era, with cyberattacks becoming increasingly rampant and intricate, a plethora of emerging technologies continually emerge to confront and mitigate evolving security challenges. This article will delve into three primary trends in future network security risk control: zero-trust architecture, the ramifications of quantum computing, and the proliferation of intelligent security solutions [43]. Firstly, zero-trust architecture has emerged as a pivotal concept in network security. Historically, there has been a tendency to perceive internal networks as relatively secure, often resulting in lenient security protocols within them. However, with the ongoing advancement of cyberattack methodologies, internal network security faces escalating threats. Zero-trust architecture advocates for a "never trust, always verify" approach, mandating stringent identity authentication and access control even within internal networks. As zero-trust architecture gains wider adoption, enterprises and organizations will prioritize monitoring and managing internal network traffic while finely controlling user identities and access permissions, ultimately fortifying overall network security [44]. Secondly, the evolution of quantum computing will significantly impact network security. Quantum computing's unique properties hold the potential to circumvent traditional encryption techniques, posing challenges to existing network security infrastructure [45]. The advent of quantum computing may compromise the security of current encryption algorithms, necessitating the development of new encryption methods resilient to quantum computing. As quantum computing matures and enters commercialization, the network security domain will necessitate continual innovation and breakthroughs to tackle emerging security challenges. Lastly, the extensive integration of artificial intelligence (AI) and machine learning (ML) technologies will be a prominent trend in future network security [46]. With the proliferation of big data and enhanced computing capabilities, AI and ML have emerged as potent tools in network security. These technologies can analyze vast datasets, detect network threats in real-time, and swiftly respond, aiding organizations in promptly identifying and mitigating security incidents. As AI and ML technologies advance further, the network security landscape will witness the introduction of more intelligent and efficient security solutions. Future trends in network security risk control will primarily revolve around zero-trust architecture, the implications of quantum computing, and the advancement of intelligent security solutions [47]. With ongoing technological development and innovation, the network security domain will encounter both challenges and opportunities [48]. Continuous learning and adaptation are essential to ensuring the sustained progression and enhancement of network security [49-52].

5. Conclusion

Network security is constantly evolving, facing challenges from technology, personnel, and regulations. Continuous technological development, enhanced user awareness, and refined laws are essential to addressing cybersecurity threats. The future of network security requires a comprehensive approach, considering both technological advancements and human behavior.

The adoption of zero-trust architecture is a key trend in network security risk control. Traditional perimeter-based defenses are no longer sufficient against sophisticated cyber attacks and insider threats. Zero-trust architecture emphasizes continuous authentication and authorization, regardless of users' or devices' location within the network. Implementing zero-trust principles significantly enhances security posture and mitigates internal and external threats.

Quantum computing technology presents both opportunities and challenges for network security. While it can revolutionize encryption, rendering many cryptographic algorithms obsolete, it also introduces new vulnerabilities exploitable by malicious actors. Organizations must stay informed about quantum computing developments and adjust security measures accordingly through research and development.

Human error remains a critical factor in network security risk control. Despite technological advances, human error contributes significantly to cybersecurity incidents. Investing in cybersecurity awareness training empowers users to recognize and mitigate risks, making employees the first line of defense against cyber threats. The future of network security

risk control involves embracing emerging technologies like zero-trust architecture and quantum computing, alongside addressing human factors through education and awareness initiatives. A proactive and holistic approach to cybersecurity is essential for organizations to protect themselves against evolving threats and safeguard sensitive data and assets.

Abbreviations

DDos	Distributed Denial of Service
APT	Advanced Persistent Threats
IDS	Intrusion Detection Systems
MFA	Multi-Factor Authentication
AI	Artificial Intelligence
ML	Machine Learning

Author Contributions

Xudong Sun is the sole author. The author read and approved the final manuscript.

Data Access Statement

No data generate in this manuscript.

Ethics Statement

No human and another animal experiment in this manuscript.

Funding Statement

No funding statement disclosure in this manuscript.

Statement

The original manuscript was authored by Xudong Sun, and all data was provided by him.

Conflicts of Interest

No conflict of interest among the authors.

References

[1] Qi Pengyun. Research on National Defense Network Security and Data Governance [J]. Big Data, 2024, 10(03): 149-162.

[2] Cao Wensheng. Exploration of Network Security Management in Smart Campus of Higher Vocational Colleges—A Case Study of Guizhou Electronic Information Vocational and Technical College [J]. Western Quality Education, 2024, 10(09): 146-150. https://doi.org/10.16681/j.cnki.wcqe.202409032

[3] Jia Long. Current Situation and Protection Strategy of Hospital Network Security under Internet Medical Mode [C]//Metallurgical Industry Education Resources Development Center. Proceedings of the Fourth Steel Industry Digital Education and Training Seminar. Second People's Hospital of Kashgar Region; 2024: 3. https://doi.org/10.26914/c.cnkihy.2024.003290

[4] Xiong Xin. Research on Computer Network Security Defense System Based on Big Data and Artificial Intelligence Technology [C]//China Cultural Information Association, Professional Committee for Exchange of Educational Achievements of China Cultural Information Association. Proceedings of the 2024 Cultural Information Development Forum. Naval Engineering University; 2024: 3. https://doi.org/10.26914/c.cnkihy.2024.004511

[5] Xue Xiaoping. Theoretical Interpretation and Practical Approach of Ideological and Political Security Education in Ethnic Minority Colleges and Universities in the New Era [J]. Heilongjiang Education (Theory and Practice), 2024, (05): 40-44.

[6] Peng Lizhi, Hu Shiyuan, Zhang Jinting, et al. Reconstruction of Ecological Security Network in Central Urban Area Considering Ecological Service Value of Suburban Farmland [J/OL]. Acta Ecologica Sinica, 2024, (13): 1-15 [2024-05-28]. http://doi.org/10.20103/j.stxb.202307311645

[7] Li Zhiyi, Xiao Yong, Shen Shaowu. Analysis and Thinking on the Current Situation of Network Security Construction in Traditional Chinese Medicine Hospitals in Hubei Province [J]. Journal of Medical Informatics, 2024, 45(04): 91-96+102.

[8] L ü Lian, Xie Donggang. Automatic Detection of Communication Network Security Vulnerabilities Based on Weighted k-Nearest Neighbor [J]. Automation and Instrumentation, 2024, (04): 21-24+31. https://doi.org/10.14016/j.cnki.1001-9227.2024.04.021

[9] Yu Gaofeng, Li Dengfeng. Multi-Dimensional Preference Rating Method for Network Security Situation Awareness Considering Group Trust [J]. Control and Decision, 2024, 39(05): 1718-1726. https://doi.org/10.13195/j.kzyjc.2022.1802

[10] Li Kuansheng, Li Jiadong, Zhang Xu, et al. Research on Hospital Network Security Closed-loop Management Mode under the Background of Smart Hospital Construction [J]. Modern Hospital Management, 2024, 22(02): 110-113.

[11] Zhang Guohong, Jiao Xiong. Method of Dynamic Early Warning of Confidential Information Security in Large-scale Communication Networks [J]. Computer Simulation, 2024, 41(04): 387-390+440.

[12] Long Yong. Research on Computer Teaching Method and Network Security Based on Project Teaching Method—Review of "Computer Teaching and Network Security Management" [J]. Applied Chemical Industry, 2024, 53(04): 1006. https://doi.org/10.16581/j.cnki.issn1671-3206.2024.04.010

[13] He Yinjie, Li Chenxin, Wei Chunxian. Research on Mine Network Security System Based on Boundary Isolation and System Protection [J]. Industrial Automation of Mining and Metallurgy, 2024, 50(03): 14-21. https://doi.org/10.13272/j.issn.1671-251x.2023100008

[14] Huang Zhiyong, Lin Renming, Liu Hong, et al. Fusion Model of Multi-source Network Security Data Based on DS Evidence Theory [J]. Modern Electronics Technology, 2024, 47(07): 115-121. https://doi.org/10.16652/j.issn.1004-373x.2024.07.020

[15] Ru Suyan. Characteristics, Risks, and Public Policy Choices of Artificial Intelligence Activities from the Perspective of Network Social Security [J]. Journal of Guangzhou Institute of Socialism, 2024, (01): 110-116.

[16] Zhao Dongmei, Sun Mingwei, Su Mengyue, et al. Network Security Situation Assessment Based on Improved SKNet-SVM [J]. Journal of Applied Sciences, 2024, 42(02): 334-349.

[17] Zhou Ruijue. Logic of Compensation for Loss of Network Security Loss Insurance and Determination of Insurance Liability [J]. Journal of Jinan University (Philosophy and Social Sciences Edition), 2024, 46(02): 149-164.

[18] Su Shan, Zhang Guanzhu, Li Guoxin, et al. Dynamic Identification Method of Network Information Transmission Security Threats Based on Greedy Iterative Algorithm [J]. Automation and Instrumentation, 2024, (03): 87-90+96. https://doi.org/10.14016/j.cnki.1001-9227.2024.03.087

[19] Du Yuhong, Hou Shouming. Risk Level Assessment Method of Optical Communication Network Security Based on Edge Computing [J]. Laser Journal, 2024, 45(03): 209-213. https://doi.org/10.14016/j.cnki.jgzz.2024.03.209

[20] Li Jing. Architectural Design of Information Security System Based on Computer Technology [J]. Information Technology and Informatization, 2024, (03): 188-191.

[21] Wei Min. Research on Network Security Construction of Railway Communication Comprehensive Network Management System [J]. Railway Communication and Signal Engineering Technology, 2024, 21(03): 42-46+88.

[22] Zhang Aijun, Zong Yaning. Negative Bias of Communication: Identification and Disposal of Network Political Security Risks [J]. Journal of Harbin Institute of Technology (Social Sciences Edition), 2024, 26(02): 34-42. https://doi.org/10.16822/j.cnki.hitskb.2024.02.003

[23] Gong Wenbo. Compliance Obligations for Network Platforms to Handle Personal Information and Paths to Crime [J]. Journal of East China University of Political Science and Law, 2024, 27(02): 52-66.

[24] Zhang Tingting, Wang Zhiqiang. Simulation of Network Security Situation Awareness Based on Backpropagation Algorithm [J]. Computer Simulation, 2024, 41(03): 436-440.

[25] Tang, Guangyan. Analysis of Network Security Measures for IP-based System Construction."Broadcasting & Television Information 31.03 (2024): 105-107. https://doi.org/10.16045/j.cnki.rti.2024.03.021

[26] Ding, Zixuan, and Chen Guo. Internal Network Security Threat Detection Method Based on XGBoost Algorithm. Journal of Jilin University (Information Science Edition) 42.02 (2024): 366-371. https://doi.org/10.19292/j.cnki.jdxxp.2024.02.016

[27] Zhang, Yinghui. Analysis on Optimization Strategy of Enterprise Network Security Organization Management System. China Intelligent Transportation 2024.03 (2024): 28-30. https://doi.org/10.13439/j.cnki.itsc.2024.03.003

[28] Yang, Fan, Ding Zhi, Wang Yang, et al. Industrial Control Network Security Protection System Based on SDN and Ensemble Learning. Modern Electronics Technique 47.06 (2024): 22-26. https://doi.org/10.16652/j.issn.1004-373x.2024.06.004

[29] Lu, Jie. Integrated Network Security Operation Solution Based on Universities. Jiangxi Communication Science & Technology 2024.01 (2024): 49-51. https://doi.org/10.16714/j.cnki.36-1115/tn.2024.01.008

[30] Chen, Gongping, and Wang Hong. Communication Network Security Situation Prediction Technology Based on Big Data Clustering. Journal of Huaiyin Normal University (Natural Science Edition) 23.01 (2024): 20-26. https://doi.org/10.16119/j.cnki.issn1671-6876.2024.01.006

[31] Zhou, Ruijue. Intervention Path of Cybersecurity Insurance in Data Leakage Risk Governance. Northern Methodology 18, no. 02 (2024): 76-90. https://doi.org/10.13893/j.cnki.bffx.2024.02.010

[32] Shi, Lingshan. Active Obligation, Criminalization, and Governance of Information Network Crime. Law Review 42, no. 02 (2024): 112-121. https://doi.org/10.13415/j.cnki.fxpl.2024.02.011

[33] Chang, Zuguo. Construction of Security Protection System for Broadcasting and Television Networks in the Smart Radio and Television Field." Television Technology 48, no. 03 (2024): 180-182. https://doi.org/10.16280/j.videoe.2024.03.049

[34] Yan, Tanglin. "Design of Intelligent Broadcasting and Television Network Security Dispatching Early Warning Architecture Based on Situation Awareness Technology. Television Technology 48, no. 03 (2024): 189-192+205. https://doi.org/10.16280/j.videoe.2024.03.052

[35] Zhang, Shuo. Analysis of Criminal Protection of Network Data Security. Legal Review (2024), no. 06: 46-48.

[36] Chen, Lu, Hui Li, and Chang Liu. Research on Security Audit System of 5G-R Network Based on eBPF and ConvLSTM. Railway Standard Design 68, no. 04 (2024): 203-210. https://doi.org/10.13238/j.issn.1004-2954.202312150001

[37] Hu, Chunhui, and Jianfeng Chen. Mechanism and Development Strategy of Frontiers of Network Security Technology. National Defense Science and Technology 45, no. 01 (2024): 87-93. https://doi.org/10.13943/j.issn1671-4547.2024.01.12

[38] Zeng, Xiaowan, Haijun Wang, Lei Huang, et al. Algorithm for Resource Allocation of Security Communication in UAV-Assisted D2D Communication Network. Journal of Communications 45, no. 02 (2024): 115-126.

[39] Zhang, Jia, Jian Han, and Jinyu Han. Situation Awareness of Laser Sensor Network Security under Logistic Regression Model. Laser Journal 45, no. 02 (2024): 174-180. https://doi.org/10.14016/j.cnki.jgzz.2024.2.174

[40] Xiao, Zhenhuai. Challenges and Countermeasures of Network Data Security Protection in Smart Education Environment of Universities. Journal of Wuhan Shipbuilding College 23, no. 01 (2024): 7-11+23.

[41] Li, L. (2024). Instant Messaging Network Security Vulnerability Identification Method Based on Dependency Search Tree. Information Technology and Informatization, (02), 151-154.

[42] Yang, Y., Yang, Y., Shu, H., et al. (2024). Research on the Path of Network Security Education for College Students from the Perspective of Ideological and Political Education. China Educational Technology Equipment, (04), 21-23+30.

[43] Guo, M. (2024). Research on Key Technologies of Network Security for Medical Equipment Based on IEC TR 60601-4-5. Instrumentation Standardization and Metrology, (01), 1-4.

[44] Ran, X. (2024). Analysis of Computer Network Security Management and Maintenance Measures. Electronic Components and Information Technology, 8(02), 179-181+185. https://doi.org/10.19772/j.cnki.2096-4455.2024.2.044

[45] Cui, B., & Yang, L. (2024). Dissemination Strategy of Advocating International Norms in Cyberspace by Science and Technology Enterprises—Taking Microsoft's Practice of International Network Security Norms as an Example. Future Communication, 31(01), 9-20+124. https://doi.org/10.13628/j.cnki.zjcmxb.2024.01.010

[46] Su, H., Liu, Y., Li, G., et al. (2024). Research on the Construction of Industrial Control System Network Security Protection System. Automation Instrumentation, 45(02), 111-115. https://doi.org/10.16086/j.cnki.issn1000-0380.2022100036

[47] Yang, D. (2024). Network Ideological Security in Colleges and Universities from the Perspective of Overall National Security Concept: Connotation, Methods, and Countermeasures. Party and Government Cadres Journal, (02), 42-49.

[48] Zhang, W. (2024). Analysis of Computer Network Security Issues and Countermeasures—Evaluation of Computer Network Security Experimental Guide. China Security Science Journal, 34(02), 250.

[49] Yang, Z., & Li, L. (2024). Research on the Security Development of Communication Network Technology in the New Era—Evaluation of Communication Network Security. China Security Science Journal, 34(02), 252.

[50] Wang, K., Yang, C., & Zhu, L. (2024). Research on Network Security Protection Strategy Based on Penetration Testing. Broadcasting & Television Information, 31(02), 106-110. https://doi.org/10.16045/j.cnki.rti.2024.02.030

[51] Luo, K., & Xu, J. (2024). The Origin, Logic, and Path of Building a Community of Shared Future in Cyberspace Security. Modern Communication (Journal of Communication University of China), 46(02), 119-128. https://doi.org/10.19997/j.cnki.xdcb.2024.02.015

[52] Qian, Z., & Zhu, T. (2024). Application of Big Data Technology in Computer Network Information Security Issues—Evaluation of Computer Network Information Security. Applied Chemical Industry, 53(02), 511. https://doi.org/10.16581/j.cnki.issn1671-3206.2024.02.015